The Mathematics Enthusiast

Volume 6
Number 1 *Numbers 1 & 2*

Article 13

1-2009

THE ORIGINS OF THE GENUS CONCEPT IN QUADRATIC FORMS

Mark Beintema

Azar Khosravani

THE ORIGINS OF THE GENUS CONCEPT IN QUADRATIC FORMS

Mark Beintema[1] & *Azar Khosravani*[2]
College of Lake County, Illinois *Columbia College Chicago*

ABSTRACT: We present an elementary exposition of genus theory for integral binary quadratic forms, placed in a historical context.

KEY WORDS: Quadratic Forms, Genus, Characters
AMS Subject Classification: 01A50, 01A55 and 11E16.

INTRODUCTION: Gauss once famously remarked that "mathematics is the queen of the sciences and the theory of numbers is the queen of mathematics". Published in 1801, Gauss' *Disquisitiones Arithmeticae* stands as one of the crowning achievements of number theory. The theory of binary quadratic forms occupies a large swath of the *Disquisitiones*; one of the unifying ideas in Gauss' development of quadratic forms is the concept of genus. The generations following Gauss generalized the concepts of genus and class group far beyond what Gauss had done, and students approaching the subject today can easily lose sight of the basic idea.

Our goal is to give a heuristic description of the concept of genus – accessible to those with limited background in number theory – and place it in a historical context. We do not pretend to give the most general treatment of the topic, but rather to show how the idea originally developed and how Gauss' original definition implies the more common definition found in today's texts.

1 2
,
Mark Beintema
Department of Mathematics
College of Lake County
19351 W. Washington Ave.
Grayslake, IL 60030
(847) 543-2913
markbeintema@clcillinois.edu

Azar Khosravani
Science and Math Department
Columbia College Chicago
600 S. Michigan Ave.
Chicago, IL 60605
(312) 344-7285
akhosravani@colum.edu

The Montana Mathematics Enthusiast, **ISSN 1551-3440, Vol. 6, nos.1&2**, pp.137- 150

BASIC DEFINITIONS: An integral binary quadratic form is a polynomial of the type $f(x,y) = ax^2 + bxy + cy^2$, where *a, b,* and *c* are integers. A form is *primitive* if the integers *a, b,* and *c* are relatively prime. Note that any form is an integer multiple of a primitive form. Throughout, we will assume that all forms are primitive. We say that a form f represents an integer *n* if $f(x,y) = n$ has an integer solution; the representation is *proper* if the integers x, y are relatively prime. A form is *positive definite* if it represents only positive integers; we will restrict our discussion to positive definite forms.

The *discriminant* of $f = ax^2 + bxy + cy^2$ is defined as $\Delta = b^2 - 4ac$. Observe that $4af(x,y) = (2ax + by)^2 - \Delta y^2$. Thus, if $\Delta < 0$, the form represents only positive integers or only negative integers, depending on the sign of a. In particular, if $\Delta < 0$ and $a > 0$ then $f(x,y)$ is positive definite. Moreover, $\Delta = b^2 - 4ac$ implies that $\Delta \equiv b^2 \pmod 4$. Thus we have $\Delta \equiv 0 \pmod 4$ or $\Delta \equiv 1 \pmod 4$, depending on whether *b* is even or odd. Moreover, we will write $(Z/\Delta Z)^*$ to denote the multiplicative group of congruence classes which are relatively prime to Δ.

We say that an integer *a* is a quadratic residue of *p* if $x^2 \equiv a \pmod p$ has a solution. When discussing quadratic residues, it is convenient to use Legendre symbols. If *p* is an odd prime and *a* an integer relatively prime to *p*, then $\left(\frac{a}{p}\right)$ is defined as follows:

DEFINITION: $$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } x^2 \equiv a \pmod p \text{ has a solution} \\ -1 & \text{otherwise} \end{cases}$$

This notation allows us to concisely state some well-known facts about quadratic residues; here *p*, *q* are distinct odd primes:

i) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ ii) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$

iii) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$ iv) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

Item (iii) is called the Quadratic Reciprocity Law; discovered independently by Euler and Legendre, the first correct proof appeared in Gauss' *Disquisitiones*. Items (i) and (ii) are known as the First and Second Supplements to Quadratic Reciprocity and were proved by Euler (1749) and Legendre (1785) respectively.

More generally, let $m = p_1 p_2 \cdots p_k$, and let a be any positive integer. The Jacobi symbol is defined as $\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right)$. Observe that if a is a quadratic residue modulo m, then $\left(\frac{a}{m}\right) = 1$, but the converse is not true. The Jacobi symbol has many of the same basic properties as the Legendre symbol; in particular the four results above are valid when p and q are replaced by arbitrary odd integers. The Jacobi symbol also satisfies $\left(\frac{a}{m}\right)\left(\frac{a}{n}\right) = \left(\frac{a}{mn}\right)$. The reciprocity law for Jacobi symbols was also proved by Gauss [**7**, Art 133], and can be stated as follows: If m and n are odd integers, then $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$ if either of $m, n \equiv 1 \pmod 4$ and $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$ if $m \equiv n \equiv 3 \pmod 4$.

HISTORICAL BACKGROUND: The earliest investigations concerning the representation of integers by binary quadratic forms were due to Fermat. In correspondence to Pascal and Marsenne, he claimed to have proved the following:

THEOREM 1:

1. Every prime number of the form $4k + 1$ can be represented by $x^2 + y^2$.
2. Every prime number of the form $3k + 1$ can be represented by $x^2 + 3y^2$.
3. Every prime number of the form $8k + 1$ or $8k + 3$ can be represented by $x^2 + 2y^2$.

These results motivated much later research on arithmetic quadratic forms by Euler and Lagrange. Beginning in 1730, Euler set out to prove Fermat's results; he succeeded in proving (1) in 1749 (as well as the more general Two-Square Theorem), and made significant progress on the other two [**1**]. In a 1744 paper titled *Theoremata circa*

divisors numerorum in hac forma $paa \pm qbb$ *contentorum*, Euler recorded many examples and formulated many similar conjectures (presented as theorems). It was in this paper that he also established many basic facts about quadratic residues. His most general result along these lines was the following:

THEOREM 2: Let n be a nonzero integer, and let p be an odd prime relatively prime to n. Then $p \mid x^2 + ny^2,\ \gcd(x, y) = 1 \iff \left(\frac{-n}{p}\right) = 1.$

In 1773, Lagrange published the landmark paper "*Recherches d'arithmetique*", in which he succeeded in proving Fermat's conjectures concerning primes represented by the forms $x^2 + 2y^2$ and $x^2 + 3y^2$. The same paper contains a general development of the theory of binary quadratic forms, treating forms of the type $f = ax^2 + bxy + cy^2$. Lagrange's development of the theory is systematic and rigorous – it is here that he introduces the crucial concepts of discriminant, equivalence, and reduction. One of the first results is a connection between quadratic residues and the representation problem for general quadratic forms:

THEOREM 3: Let m be a natural number that is represented by the form $ax^2 + bxy + cy^2$. Then $\Delta = b^2 - 4ac$ is a quadratic residue modulo m.

One of Lagrange's primary innovations was the concept of equivalence of forms (although the terminology is due to Gauss). We say that two forms are *equivalent* if one can be transformed into the other by an invertible integral linear substitution of variables. That is, f and g are equivalent if there are integers $p, q, r,$ and s such that $f(x, y) = g(px + qy, rx + sy)$ and $ps - qr = \pm 1$. It can be shown (e.g. see [**6**] or [**11**]) that equivalence of forms is indeed an equivalence relation. Moreover, equivalent forms have the same discriminant and represent the same integers (the same is true for proper representation). Gauss later refined this idea by introducing the notion of proper equivalence. An equivalence is a proper equivalence if $ps - qr = 1$, and it is an improper equivalence if $ps - qr = -1$. Following Gauss, we will say that two forms are in the same class if they are properly equivalent. Using these ideas, we obtain the following

partial converse of Theorem 3:

THEOREM 4: Let p be an odd prime. Then p is represented by a form of discriminant Δ if and only if $\left(\frac{\Delta}{p}\right)=1$.

Proof: Let $f=ax^2+bxy+cy^2$ represent p, say $p=ar^2+brs+cs^2$. Because p is prime, we must have gcd(r, s) = 1. Hence, we can write $1=ru-st$ for integers t, u. If $g(x,y)=f(rx+ty, sx+uy)$, then g is properly equivalent to f and thus has discriminant Δ. Moreover, by direct calculation we have $g=px^2+b'xy+c'y^2$. Thus, $\Delta=b'^2-4pc'$ and so $b'^2\equiv\Delta \pmod p$. Next, suppose that $m^2\equiv\Delta \pmod p$. We can assume that m has the same parity as Δ (replacing m by $m + p$ if necessary). Writing $m^2-\Delta=kp$, and recalling that $\Delta\equiv 0$ or $1 \pmod 4$, we have $kp\equiv 0 \pmod 4$. Thus the form $px^2+mxy+(k/4)y^2$ has integer coefficients and represents p

Once we have partitioned the set of binary quadratic forms into equivalence classes, the next logical step is to choose an appropriate representative for each class. This naturally leads another of Lagrange's innovations, the concept of reduction. A primitive positive definite form $ax^2+bxy+cy^2$ is said to be *reduced* if $|b|\le a\le c$ and $b\ge 0$ if either $|b|=a$ or $a=c$. Lagrange showed that every primitive positive definite form is properly equivalent to a unique reduced form, and that there are only there are only finitely many positive definite forms with a given determinant Δ **[6, 11]**. We write $h(\Delta)$ for the number of classes of primitive positive definite forms of discriminant Δ. Thus, $h(\Delta)$ is the number of reduced forms of discriminant Δ.

In the special case where $h(-4n)=1$, the only reduced form of discriminant -4n will be the form x^2+ny^2. In this case, $p=x^2+ny^2 \Leftrightarrow \left(\frac{-n}{p}\right)=1$. This situation is in fact quite rare – Gauss conjectured that the only values of n for which $h(-4n)=1$ are n = 1, 2, 3, 4, and 7. The conjecture was proved by Landau in 1903. More generally,

we call Δ a *fundamental discriminant* if it cannot be written as $\Delta = k^2\Delta_0$, where $k > 1$ and $\Delta_0 \equiv 0$ or $1 \pmod 4$. Gauss conjectured that if $\Delta < 0$ is a fundamental discriminant then $h(\Delta) = 1$ only for Δ = -3, -4, -7, -8, -11, -19, -43, -67, -163. This was proved in 1952 by Heegner [**12**].

GENUS THEORY: We say that two primitive positive definite forms of discriminant Δ are in the same *genus* if they represent the same values in $(Z/\Delta Z)^*$. Recall that equivalent forms represent the same integers and so must be in the same genus. Thus, the concept of genus provides a method of separating reduced forms of the same discriminant according to congruence classes represented by the forms. In his table of reduced forms, Lagrange showed forms grouped according to the congruence classes represented by the forms. For this reason, many authors credit the original idea of genus to Lagrange. Some authors have even attributed the idea to Euler [**10**]. However, Gauss is the first to explicitly discuss the concept of genus. More importantly, he is the first to put it to use.

Before presenting Gauss' definition of genus, a few remarks concerning notation and terminology are in order. Throughout most of the *Disquisitiones Arithmetica*, Gauss assumes forms have even middle coefficient – that is, he mostly considers forms of type $ax^2 + 2bxy + cy^2$. (Forms with odd middle coefficient are called "improperly primitive", and are treated separately.) Instead of discriminants, he uses the *determinant* of the form, defined as $D = b^2 - ac$. Note that the discriminant Δ satisfies $\Delta = 4D$.

The following result, found in Article 229 of *Disquisitiones Arithmetica*, is the foundation of genus theory. The proof is paraphrased slightly from the original text.

THEOREM 5: Let F be a primitive form with determinant D and p a prime number dividing D: then the numbers not divisible by p which can be represented by the form F agree in that they are either all quadratic residues of p, or they are all nonresidues.

Proof: Let $m = ag^2 + 2bgh + ch^2$ and $m' = ag'^2 + 2bg'h' + ch'^2$. Then

$$mm' = [agg' + b(gh' + hg') + chh']^2 - D(gh' - hg')^2.$$

Thus mm' is a quadratic residue mod D, and hence is also a quadratic residue mod p for any p dividing D. It follows that m, m' are either both residues, or both are non-residues mod p. That is, if m and m' are both represented by F, then $\left(\frac{m}{p}\right)=\left(\frac{m'}{p}\right)$ □

From the relation $\Delta = 4D$ we get two important observations: First, any odd prime that divides D also divides Δ. Moreover, if p is an odd prime, then Δ is a residue mod p if and only if D is. Thus Theorem 5 still holds if the word determinant is replaced by discriminant. Henceforth, we will revert to the more common practice of using discriminants.

The argument used to prove Theorem 5 also shows that if $8 \mid D$ or $4 \mid D$, then the product of two numbers represented by F will be a quadratic residue mod 8 or a quadratic residue mod 4, respectively. Hence if $8 \mid D$, then exactly one of the following is true: all numbers represented by F are $\equiv 1 \pmod 8$, or all are $\equiv 3 \pmod 8$, or all are $\equiv 5 \pmod 8$, or all are $\equiv 7 \pmod 8$. Likewise, if $4 \mid D$, but $8 \nmid D$, then all numbers represented by F are $\equiv 1 \pmod 4$, or all are $\equiv 3 \pmod 4$.

These observations are then used to classify forms according to *characters*. Let $p_1, p_2, ..., p_k$ be the odd prime divisors of D. Define $\chi_i = Rp_i$ if the numbers represented by F are quadratic residues of p_i, and $\chi_i = Np_i$ if the numbers represented by F are quadratic non-residues of p_i. We define one additional character, χ_0, which will be an ordered pair a, b chosen from the list {(1,4), (3,4), (1,8), (3,8), (5,8), (7,8)}, where all numbers m represented by the form f satisfy $m \equiv a \pmod b$. For example, we write $\chi_0 = 1,4$ to indicate that all numbers represented by the form are congruent to 1 mod 4. Finally, the *complete character* for a form is then defined as: $\chi_0; \chi_1, \chi_2, ..., \chi_k$. Two forms then said to be in the same *genus* if they have the same complete character.

In Article 231, Gauss discusses the possibilities for χ_0 based on the prime factorization of the determinant, as well as the number of potential complete characters in each case. In each case, the number of potential complete characters is a power of 2.

Let $p_1 p_2 \cdots p_k$ be all of the odd primes dividing Δ. We summarize the results in the table below:

Δ	Possible χ_0	Number of potential complete characters
$\Delta = 8 \cdot 2^r \cdot p_1 p_2 \cdots p_k$ $(r \geq 0)$	1,8 3,8 5,8 7,8	2^{k+2}
$\Delta = 4 \cdot p_1 p_2 \cdots p_k$	1,4 3,4	2^{k+1}
$\Delta = p_1 p_2 \cdots p_k \equiv 1 \pmod 4$	1,4	2^k

Table 1

EXAMPLE: Let $\Delta = -55$; then χ_0 = 1,4 and there are four reduced forms:

$$f_1 = x^2 + xy + 14y^2, \quad f_2 = 2x^2 + xy + 7y^2$$
$$f_3 = 2x^2 - xy + 7y^2, \quad f_4 = 4x^2 + 3xy + 4y^2$$

f_1 represents 1, and 1 is a residue for any prime *p*, so the complete character for f_1 is 1,4; *R*5, *R*11. f_2 and f_3 each represent 2, which is a non-residue mod 5 and mod 11, so the complete character for each of these forms is 1,4; *N* 5, *N*11. Finally, f_4 represents 4, which is a residue modulo any odd prime *p*. Thus the complete character for f_4 is *R*5, *R*11.

It follows that there are two genera, each with two proper equivalence classes:

Complete Character	Reduced Forms
1,4; *R*5, *R*11	$f_1 = x^2 + xy + 14y^2, \quad f_4 = 4x^2 + 3xy + 4y^2$
1,4; *N* 5, *N*11	$f_2 = 2x^2 + xy + 7y^2, \quad f_3 = 2x^2 - xy + 7y^2$

Note that f_2, f_3 are equivalent, so they must be in the same genus. However, they are *not* properly equivalent since $f_3 = f_2(-x, y)$. Thus they represent two distinct elements within the genus.

Observe also that in the example above, there were four possible complete characters, but only two actually defined a genus. In Articles 261 and 287, Gauss

shows that the number of genera is always exactly half the number of possible complete characters and must always be a power of 2. For odd, non-square discriminants, this is easy to see: Let m be an odd integer represented by a form f of odd discriminant Δ, and let p be an odd prime dividing Δ. If Rp is a character, then $\left(\frac{m}{p}\right)=1$, whereas if Np is a character, then $\left(\frac{m}{p}\right)=-1$. Replacing the characters by their respective Legendre symbols and multiplying, we get $\left(\frac{m}{p_1}\right)\left(\frac{m}{p_2}\right)\cdots\left(\frac{m}{p_k}\right)=\left(\frac{m}{\Delta}\right)$, where $\left(\frac{m}{\Delta}\right)$ is the Jacobi symbol and $\Delta = p_1 p_2 \cdots p_k$. By reciprocity we have $\left(\frac{m}{\Delta}\right)=(-1)^{(m-1)(\Delta-1)/4}\left(\frac{\Delta}{m}\right)$. Since m is odd and $\Delta \equiv 1 \pmod 4$, we have $\left(\frac{m}{\Delta}\right)=\left(\frac{\Delta}{m}\right)$. Finally, since m is represented by f, we have $\left(\frac{\Delta}{m}\right)=1$ by Theorem 3. Thus, for m represented by f, the product of the characters is always 1; if $k-1$ of the characters are known, the k-th is also determined. It follows that there must be 2^{k-1} complete characters.

Reciprocity plays a critical role in the argument above, and this is no accident. In Article 261, Gauss shows that at least half the possible complete characters cannot belong to a genus – this fact serves as the basis of his second proof of the Quadratic Reciprocity [**7**, Art 262].

The argument above (or Theorem 3) shows that if m is represented by a form of odd discriminant Δ, then $\left(\frac{\Delta}{m}\right)=1$. Gauss' Theorem 5 then allows us to extend this relationship to elements of $(Z/\Delta Z)^*$. That is, $\chi(\overline{m})=\left(\frac{\Delta}{m}\right)$ is a well-defined map from $(Z/\Delta Z)^*$ to $\{\pm 1\}$. This is a homomorphism since $\left(\frac{\Delta}{m}\right)\left(\frac{\Delta}{n}\right)=\left(\frac{\Delta}{mn}\right)$. Moreover, this is the *unique* homomorphism $\chi:(Z/\Delta Z)^* \to \{\pm 1\}$ such that $q \in \ker(\chi)$ if and only if q is represented by a form of discriminant Δ. A famous result of Dirichlet guarantees that there are infinitely many primes in an arithmetic progression, provided the first term and

common difference are relatively prime. Thus, each element of $(Z/\Delta Z)^*$ can be represented as $\overline{q}$, for some odd prime q not dividing Δ. From this, it follows that the the condition $\chi(\overline{q}) = \left(\frac{\Delta}{q}\right)$ for odd primes q determines χ uniquely.

Let $\Delta \equiv 0, 1 \pmod 4$ be a discriminant. The *principal form* is defined by

$$x^2 - \frac{\Delta}{4}y^2 \quad \textit{if} \quad \Delta \equiv 0 \pmod 4$$

$$x^2 + xy + \frac{1-\Delta}{4}y^2 \quad \textit{if} \quad \Delta \equiv 1 \pmod 4$$

The class and genus containing the principal form are called the *principal class* and *principal genus*, respectively. Note that the principal form has discriminant Δ and is reduced. When $\Delta = -4n$, the principal form is $x^2 + ny^2$. Many fundamental properties of genus can be described in terms of the homomorphism χ and the principal form:

THEOREM 6: Given a negative integer $\Delta \equiv 0, 1 \pmod 4$, let χ be the homomorphism of Theorem 4, and let f be a form of discriminant Δ.

i) For an odd prime not dividing Δ, $\overline{p} \in \ker(\chi)$ if and only if p is represented by one of the $h(\Delta)$ forms of discriminant Δ.
ii) $\ker(\chi)$ is a subgroup of index 2 in $(Z/\Delta Z)^*$
iii) The values in $(Z/\Delta Z)^*$ represented by the principal form of discriminant Δ form a subgroup $H \subset \ker(\chi)$
iv) The values in $(Z/\Delta Z)^*$ represented by $f(x, y)$ form a coset of H in $\ker(\chi)$.
v) For odd Δ, $H = \{x^2 \mid x \in (\mathbf{Z}/\Delta\mathbf{Z})^*\}$

Part (i) of the theorem is a restatement of Theorem 3: $\chi(\overline{p}) = \left(\frac{\Delta}{p}\right) = 1$ if and only if p is represented by some form of discriminant Δ. Part (ii) states that exactly half the congruence classes in $(Z/\Delta Z)^*$ are represented by some form of discriminant Δ; for odd Δ, this follows from our argument that exactly half of all possible complete characters actually result in a genus. Parts (iii) and (iv) get to the heart of genus theory; since distinct cosets are disjoint, different genera represent disjoint classes in $(Z/\Delta Z)^*$. That is, we can now describe genera in terms of cosets kH of H in $Ker(\chi)$. We could then

define a genus to consist of all forms of discriminant Δ that represent the values of kH mod Δ. Note that this definition could be used to show that each genus contains the same number of classes [**9**, Art. 252].

EXAMPLE: Recall that there were four reduced forms of discriminant Δ = - 55:

$$f_1 = x^2 + xy + 14y^2, \quad f_2 = 2x^2 + xy + 7y^2$$
$$f_3 = 2x^2 - xy + 7y^2, \quad f_4 = 4x^2 + 3xy + 4y^2$$

There are $\Phi(55) = 55(1-\frac{1}{5})(1-\frac{1}{11}) = 40$ elements in $(Z/55Z)^*$. Of these 40 elements, exactly 20 are represented by a form of discriminant -55.

Since $f_1(x,0) = x^2$, the principal form $f_1 = x^2 + xy + 14y^2$ represents all of the squares:

$$H = \{1, 4, 9, 14, 16, 26, 31, 34, 36, 49\}$$

Thus the set of classes in $(Z/55Z)^*$ represented by f_1, f_4 is H, which is easily verified to be a subgroup of $(Z/55Z)^*$. Also note that $f_2(0,y) = 7y^2$, so the set of classes represented by f_2, f_3 can be written as $7H = \{2, 7, 8, 13, 17, 18, 28, 32, 43, 52\}$.

Of special interest are those discriminants Δ such that each genus contains exactly one class; in this situation, the primes that are represented by a form of discriminant Δ are determined by congruence conditions mod Δ. (See [**2**] for details.)

COMPOSITION OF FORMS: The theory of composition is intricately linked to that of genus. Composition of forms was first investigated by Legendre and Lagrange, but the theory was brought to fruition by Gauss, who discovered a remarkable group structure. Gauss' exposition is long and technical, and is one of the most difficult parts of the *Disquisitiones*. However, the main result – that classes of binary quadratic forms of fixed discriminant form an abelian group under the operation of composition – is justly celebrated as one of the milestones of 19th century mathematics. Mathematicians following Gauss were able to streamline the theory considerably.

Gauss showed that any two forms of the same discriminant can be composed in such a way that composition is a well-defined operation on (proper) equivalence classes of forms. For simplicity, we present a version of the operation developed by Dirichlet [**2,**

3] which is based on a case singled out by Gauss for special consideration [**7**, Art 242]. We say that $f_1 = a_1x^2 + b_1xy + c_1y^2$ and $f_2 = a_2x^2 + b_2xy + c_2y^2$ are *concordant* (the terminology is due to Dedekind [**3**]) if the following conditions hold:

i) $a_1a_2 \neq 0$ ii) $b_1 = b_2$ iii) $a_1 \mid c_2$ and $a_2 \mid c_1$

If two concordant forms have the same discriminant, say $b^2 - 4a_1c_1 = b^2 - 4a_2c_2$, then $a_1c_1 = a_2c_2$, and so $c_1 / a_2 = c_2 / a_1$. We then define the composition of two concordant forms f_1, f_2 of discriminant Δ as $f_1 * f_2 = a_1a_2x^2 + bxy + cy^2$, where $b = b_1 = b_2$ and $c = c_1 / a_2 = c_2 / a_1$. Dirichlet showed that given two equivalence classes of forms C_1, C_2, it is always possible to find concordant forms f_1, f_2 with $f_1 \in C_1$ and $f_2 \in C_2$.

Suppose that $f_1 = a_1{x_1}^2 + bx_1y_1 + a_2c{y_1}^2$ and $f_2 = a_2{x_2}^2 + bx_2y_2 + a_1c{y_2}^2$ are concordant forms. Then setting $X = x_1x_2 - cy_1y_2$ and $Y = a_1x_1y_2 + a_2y_1x_2 + by_1y_2$, we have $(a_1{x_1}^2 + bx_1y_1 + a_2c{y_1}^2)(a_2{x_2}^2 + bx_2y_2 + a_1c{y_2}^2) = a_1a_2X^2 + bXY + cY^2$ (by direct calculation). Using this identity and the definition of composition given above, we quickly deduce that $f_1 * f_2$ represents m_1m_2 whenever f_1 represents m_1 and f_2 represents m_2. The following theorem summarizes the main properties of composition [**7**, Art 242]:

THEOREM 8 [Gauss]: For a fixed discriminant Δ, the set of equivalence classes of primitive positive definite forms comprise an abelian group under the operation of composition. The identity of this group is the class containing the principal form. The class containing the form $ax^2 + bxy + cy^2$ and the class containing its "opposite" $ax^2 - bxy + cy^2$ are inverses.

This group is called the *class group,* and has cardinality $h(\Delta)$. The proof is long and technical, as might be expected; the results themselves represent an unprecedented level of abstraction for their time. Soon after discussing composition of classes, Gauss defines *duplication*: let K and L be proper equivalence classes of forms of discriminant D. If $K * K = L$, then we say that L is obtained by duplication of K. In Article 247, Gauss points out that the duplication of any class lies in the principal genus; in Articles 286-287 he shows the converse, stating that

"*it is clear that any properly primitive class of binary forms belonging to the principal genus can be derived from the duplication of some properly primitive class of the same determinant*".

This fact is often referred to in the literature as the Principal Genus Theorem. While the statement is made rather casually (not even stated as a formal theorem), Gauss nonetheless describes it as "*among the most beautiful in the theory of binary forms*". (See [**12**] for a discussion of the many generalizations of this result.)

We conclude with a description of Gauss' proof of the Principal Genus Theorem. To demonstrate how duplication of any class is in the principal genus, Gauss defines composition of genera, and in doing so describes another group structure. In Article 246, he shows that if f, f' are primitive forms from one genus, and if g, g' are primitive forms from another genus, then the compositions $f * g$ and $f' * g'$ will be in the same genus. He then explains how one can determine the genus of $f * g$ using the characters for *f*, *g* respectively. First, he gives a multiplication table for the characters χ_0; then he describes multiplication of characters χ_i, χ_i' as Rp_i if $\chi_i = \chi_i'$ and as Np_i if $\chi_i \neq \chi_i'$. The characters of $f * g$ are then the products of χ_i, χ_i', $i = 0,1,...,k$. If the discriminant Δ is odd, we can illustrate this by replacing the characters by their respective Legendre symbols. Let $\Delta = p_1 p_2 \cdots p_k$ be odd, and let *f*, *g* come from the genera G_1, G_2 respectively. Suppose that *m* is represented by *f* and that *n* is represented by *g,* so the total characters of the forms can be described as $\left(\frac{m}{p_1}\right), \left(\frac{m}{p_2}\right), \cdots, \left(\frac{m}{p_k}\right)$ and $\left(\frac{n}{p_1}\right), \left(\frac{n}{p_2}\right), \cdots, \left(\frac{n}{p_k}\right)$ respectively. Then $G_1 * G_2$ is the genus with total character $\left(\frac{mn}{p_1}\right), \left(\frac{mn}{p_2}\right), \cdots, \left(\frac{mn}{p_k}\right)$. Note that the principal genus always represents 1, which is a quadratic residue modulo any prime; that is, $\left(\frac{1}{p_i}\right) = 1$ for all *i*. Thus the principal genus *G* is the genus in which all the characters have value 1. On the other hand, if G_i is any

other genus and m is an integer represented by G_i, the characters for $G_i * G_i$ will be $\left(\frac{m^2}{p_1}\right),\left(\frac{m^2}{p_2}\right),\ldots,\left(\frac{m^2}{p_k}\right) = 1, 1,\ldots, 1.$ Hence $G_i * G_i = G$. Moreover, it follows that the genera form a group of order 2, whose identity is the principal genus.

BIBLIOGRAPHY

1. M. Beintema and A. Khosravani, "Binary Quadratic Forms: A Historical View", Mathematics and Computer Education, **40** (2006), p. 226-236.
2. D.A. Cox, *Primes of the Form* $x^2 + ny^2$, Wiley-Interscience, John Wiley and Sons, New York, 1989.
3. L.E. Dickson, *Theory of Numbers Vol. III: Quadratic and Higher Forms*, Chelsea, New York, 1952.
4. L. Euler, *Oeuvres Vol II*, Gauthier-Villars and Sons, Paris, 1894.
5. P. de Fermat, *Oeuvres Vol II*, Gauthier-Villars and Sons, Paris, 1894.
6. D. Flath, *Introduction to Number Theory*, Wiley, New York, 1989.
7. C.F. Gauss, *Disquisitiones Arithmeticae*, Springer-Verlag, New York, 1986.
8. J.L. Lagrange, "Recherches d'arithmetique", *Oeuvres III*, Gauthier-Villars, Paris, 1867.
9. A.M. Legendre, *Theorie des Nombres*, Paris, 1830; reprint, Blanchard, Paris, 1955.
10. F. Lemmermeyer: "The Development of the Principal Genus Theorem", ArXiv Mathematics e-prints, math/0207306, 2002.
11. W. Scharlau and H. Opolka, *From Fermat to Minkowski, Lectures on the Theory of Numbers and Its Historical Development*, Springer-Verlag, New York, 1985.
12. J.P. Serre, $\Delta = b^2 - 4ac$, Math. Medley **13** (1985), pp. 1-10.